UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,462	11/16/2001	Owen N. Wells	30GF9132	3773

45430 7590 11/15/2007

PATRICK W. RASCHE (14983)
ARMSTRONG TEASDALE LLP
ONE METROPOLITAN SQUARE, SUITE 2600
ST. LOUIS, MO 63102-2740

EXAMINER
NGUYEN, PHUONGCHAU BA

ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
11/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/991,462	WELLS ET AL.	
	Examiner	Art Unit	
	Phuongchau Ba Nguyen	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,6-27,30,32-36,38,39,42-47,49 and 50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,6-27,30,32-36,38,39,42-47,49 and 50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 12, 14, 19, 21, 24, 25, 27, 38-39, 42, 47, 49 are rejected under 35 U.S.C. 103(s) as being unpatented over Kawase (5,631,896) in view of Lo (6,842,481).

Regarding claims 1, 15,

Kawase (5,631,896) discloses an autonomous circuit enabling the routing of data to a primary or secondary network cable connected to primary and secondary nodes (not shown-but it is inherent on the working and protection paths) comprising:

a first monitoring device (bit error detecting circuit 56-fig.3) for reporting link status of the primary network cable (working path), wherein the link status

of the primary network cable includes a notification of a fault within the primary network cable (col.7, lines 10-16);

a second monitoring device (66-fig.3) for reporting the link status of the secondary cable (protection path) and secondary node;

a logic device (correlation monitoring circuit 75-fig.3) for monitoring the link status reported by the first monitoring device (bit error detecting circuit 56-fig.3); and

a switching device (switching circuit 71-fig.3) for routing the data to one or the other of the primary or secondary network cables, wherein the first monitoring device is disconnected from monitoring the primary network cable (working path) and primary node and connected to monitoring the secondary network cable and secondary node when the switching device routes the data to the secondary network cable (protection path).

Kawase discloses all the claimed limitations, except (1) the monitoring device comprising a physical layer transceiver. However, in the same field of the endeavor, Lo (6,842,481) discloses a repeater 30 comprising a physical layer transceiver 36 in figure 2, see also figure 3 (corresponding to (1)).

Therefore, it would have been obvious to an artisan to apply Lo's teaching to Kawase's system with the motivation being to provide security in Ethernet based media independent interface communications.

Regarding claim 16,

Kawase does not explicitly disclose wherein the logic device routes the signal back to the primary network cable when the first monitoring device indicates a fault in the secondary network cable or secondary node. However, Kawase further discloses switching from working to protection path (fig.11, step sp26). Therefore, it would have been obvious to an artisan to implement backup for working path as well as protection path to use as interchangeable with the motivation being to provide protection to the backup/secondary path.

Regarding claim 12,

Kawase discloses in figure 3 wherein the only purpose of the first and second monitoring devices (bit error detecting circuits 56 & 66-fig.3) is monitoring the link status of the primary and secondary network cables

(working and protection paths) and their associated ports (not shown), and reporting the status (to the correlation monitoring circuit 75-fig.3) using a link status output associated with each of the first and second monitoring devices (bit error detecting circuits 56 & 66-fig.3).

Regarding claim 14,

Kawase further discloses wherein the logic device (correlation monitoring circuit 75-fig.3) causes the switching device (switching circuit 71-fig.3) to change the route of the data from the primary cable to the secondary cable if the first monitoring device reports a fault in the primary network cable or primary port, and the second monitoring device reports no fault in the secondary network cable or the secondary port (by sending switching control signal S21-fig.3).

Regarding claim 19,

Kawase further discloses wherein the primary and secondary network cables comprise one of: a fiber distributed data interface (FDDI), a token ring network, or an asynchronous transfer mode (ATM) (col.1, lines 9-12).

Regarding claim 21,

Kawase further discloses wherein the primary and secondary network cables connect to nodes (line terminals 1 & 2-fig.1), and not to a server.

Regarding claim 24,

Kawase further discloses wherein the circuit (figs. 2-3) comprises hardware only.

Regarding claim 25,

Kawase further discloses wherein the circuit (figs. 2-3) comprises no user configurable parameters and no firmware.

Regarding claim 27,

Kawase further discloses wherein the circuit (figs.2-3) provides electrical outputs (S7 & S17) to indicate the primary and secondary network cable status (error or not) to other equipment (correlation monitoring circuit 75-fig.3).

Regarding claim 37,

Lo further discloses wherein the first monitoring device is a physical layer transceiver (figs. 2-3, physical layer transceiver 36).

Regarding claims 35-36, 38,

Kawase (5, 631,896) discloses a method of administering a redundant cable system comprising:

monitoring, with the first monitoring device (signal failure detecting circuit 16-fig.2), an occurrence of a fault within a primary network cable (working path-fig.2)

monitoring, with second monitoring device (signal failure detecting circuit 26-fig.2), an occurrence of a fault within a second network cable (figs.9-11); and

switching a data stream route from the primary network cable to the secondary network cable when the first monitoring device indicates a fault in the primary network cable (by the switch circuit 30-fig.2, col.1, lines 54-62).

Kawase discloses all the claimed limitations, except (1) the monitoring device comprising a physical layer transceiver. However, in the same field of the endeavor, Lo (6,842,481) discloses a repeater 30 comprising a physical layer transceiver 36 in figure 2, see also figure 3 (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Lo's teaching to Kawase's system with the motivation being to provide security in Ethernet based media independent interface communications.

Kawase does not explicitly disclose wherein the logic device routes the signal back to the primary network cable when the first monitoring device indicates a fault in the secondary network cable or secondary node. However, Kawase further discloses switching from working to protection path (fig.11,

step sp26). Therefore, it would have been obvious to an artisan to implement backup for working path as well as protection path to use as interchangeable with the motivation being to provide protection to the backup/secondary path.

Regarding claim 39,

Kawase further discloses wherein the faults in the primary and secondary network cables (working and protection paths-fig.2) are indicated solely by link status outputs on each of the first and second monitoring devices (signal failure detecting circuits 16 & 26-fig.2).

Regarding claim 42,

Kawase further discloses wherein the monitoring of (the primary network cable) and switching from the primary network cable are accomplished with no programming and no software (by the switching circuit 30-fig.2).

Regarding claim 47,

Kawase (5,631,896) discloses a method of creating a cable redundancy comprising:

monitoring a primary network cable (signal failure detecting circuit 16-fig.2) and switching (by switch circuit 30-fig.2) data traveling along the primary network cable to a secondary network cable when a fault is detected in the primary network cable, wherein a link status output (failure status of the working link) on the first PHY indicates the status of the primary network cable (col.2, lines 54-62, fig.2).

Kawase discloses all the claimed limitations, except (1) the monitoring primary and secondary network cables with first and second physical layer transceivers. However, in the same field of the endeavor, Lo (6,842,481) discloses a repeater 30 comprising a physical layer transceiver 36 in figure 2, see also figure 3 (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Lo's teaching to Kawase's system with the motivation being to provide security in Ethernet based media independent interface communications.

Regarding claim 49,

Kawase further discloses the monitoring the working data link is monitored by the signal failure detecting circuit 16, see fig.2 (corresponding to "wherein the monitoring of the primary network cable is accomplished with no programming and no firmware").

3. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawase in view of Lo (6,842,481) as applied to claim 1 above, and further in view of Stener (6,690,650).

Regarding claim 50,

Kawase discloses all the claimed limitations, except (1), wherein the first monitoring device translates a message based on a speed of a network.

However, in same field of endeavor, Stener (6,690,650) discloses the network repeater performing a down shifting operation by breaking the established 100 Mb/s link, and restarting auto-negotiation to establish 10 Mb/s link, see abstract (corresponding to (1)). Therefore, it would have been

obvious to an artisan to apply Stener's teaching to provide a more reliable link incorporate two or more repeaters at different data rates and to reduce error rate to bridges, routers, interfaces and switches.

4. Claims 30, 32-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Kawase in view of Stener (6,690,650) , and further in view of Lo (6,842,481).

Regarding claim 30,

Kawase discloses a method of creating a cable redundancy comprising:

monitoring a link status of a primary network cable (working path) with a first monitoring device (signal failure detecting circuit 16-fig.2), wherein the link status of the primary network cable includes a notification of a fault within the primary network cable (col.1, lines 54-58);

monitoring a secondary network cable with a secondary monitoring device (26-fig.2), wherein the secondary monitoring device indicates the status of the secondary network device; and

switching data traveling along the primary network cable (working path) to a secondary network cable (protection path) when a fault is detected in the primary network cable (working path), wherein a link status output on the first monitoring device (i.e., failure on the working path) indicates the status of the primary network cable (figs. 9-11).

Kawase discloses all the claimed limitations, except (1), wherein the first monitoring device translates a message based on a speed of a network when the physical transceiver does not monitor the link status of the primary network cable. However, in same field of endeavor, Stener (6,690,650) discloses the network repeater performing a down shifting operation by breaking the established 100 Mb/s link, and restarting auto-negotiation to establish 10 Mb/s link, see abstract (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Stener's teaching to provide a more reliable link incorporate two or more repeaters at different data rates and to reduce error rate to bridges, routers, interfaces and switches.

Kawase does not explicitly disclose wherein the logic device routes the signal back to the primary network cable when the first monitoring device

indicates a fault in the secondary network cable or secondary node. However, Kawase further discloses switching from working to protection path (fig.11, step sp26). Therefore, it would have been obvious to an artisan to implement backup for working path as well as protection path to use as interchangeable with the motivation being to provide protection to the backup/secondary path.

Regarding claim 32,

Kawase further discloses wherein the monitoring of (the primary network cable) and switching from the primary network cable are accomplished with no programming and no software (by the switching circuit 30-fig.2).

Regarding claim 33,

Kawase further discloses monitoring the secondary network cable (protection path) with a second monitoring device (signal failure detecting circuit 26-fig.2), wherein a second link status output on the second monitoring device indicates the status of the secondary network cable (i.e., failure on the protection path, see figs.9-11).

Regarding claim 34,

Kawase discloses all the claimed limitations, except (1) wherein the second monitoring device is a physical layer transceiver.

However, in the same field of the endeavor, Lo (6,842,481) discloses a repeater 30 comprising a physical layer transceiver 36 in figure 2, see also figure 3 (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Lo's teaching to Kawase's system with the motivation being to provide security in Ethernet based media independent interface communications.

5. Claims 2-7, 9-10, 17-18, 23, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawase (5,631,896) in view of Lo (6,842,481), as applied to claim 1 above, and further in view of Bray (6,618,392).

Regarding claim 2,

Kawase discloses all the claimed limitations, except (1) the circuit (line selection device 260-fig.5a) comprises a repeater device for retransmitting data from a local network port, the repeater having at least two ports from which the

repeater device can transmit outgoing data and at least one port, which can be used for receiving incoming data .

However, in the same field of endeavor, Bray (6,618,392) discloses a repeater for retransmitting received data to all ports, see column 1, lines 22-26; fig.1 (corresponding to (1)). Therefore, it would have been obvious to apply Bray's teaching to Kawase's system with the motivation being to prevent the network from being rendered unusable by a node or path that is down.

Regarding claim 3,

Kawase further discloses a second monitoring device (error bit detecting circuit 66-fig.3) for reporting the link status of the secondary network cable (protection path) and secondary node.

Regarding claim 4,

Kawase further discloses wherein the second monitoring device is PHY (signal failure detecting circuits 16 & 26-fig.2.

Regarding claim 5,

Kawase further discloses wherein the logic device (correlation monitoring circuit 75-fig.3) monitors the link status reported by the second monitoring device (bit error detecting circuit 66-fig.3).

Regarding claim 6,

Kawase further discloses wherein the logic device (correlation monitoring circuit 75-fig.3) causes the switching device (switching circuit 71-fig.3) to change the route of the data from the primary cable to the secondary cable if the first monitoring device reports a fault in the primary network cable or primary port, and the second monitoring device reports no fault in the secondary network cable or the secondary port (by sending switching control signal S21-fig.3).

Regarding claim 7,

Kawase discloses all the claimed limitations, except (1) wherein the logic device (correlation monitoring circuit 75-fig.3) causes the switching device

(switching circuit 71-fig.3) to change the route of the data from the secondary cable (protection path) to the primary cable (working path) if the second monitoring device reports a fault in the secondary network cable or the secondary port, and the first monitoring device reports no fault in the primary network cable or the primary port. However, it would have been obvious to an artisan to implement a reversion to the working path upon a detection of error on the failure path with the motivation being to provide an efficient way to overcome the effect of failures within the network and provide fast restoration of transmission link once a failure has been detected.

Regarding claim 9,

Kawase discloses in figure 3 wherein the only purpose of the first and second monitoring devices (bit error detecting circuits 56 & 66-fig.3) is monitoring the link status of the primary and secondary network cables (working and protection paths) and their associated ports (not shown), and reporting the status (to the correlation monitoring circuit 75-fig.3) using a link

status output associated with each of the first and second monitoring devices (bit error detecting circuits 56 & 66-fig.3).

Regarding claims 10, 13,

Kawase discloses all the claimed limitations, except (1) wherein neither the first nor second monitoring device is used as an interface between a physical cable medium and a network MAC device.

However, Kawase discloses the first and second bit error detecting circuits 56 & 66-fig.3 connecting to the working and protecting paths correlation monitoring circuit 75-fig.3, thus no bit error detecting circuits used as interface between the physical cable medium and network MAC device (corresponding to (1)). Therefore, it would have been obvious to an artisan to use bit error detecting circuits to detect errors on the working and protection paths with the motivation being to provide an efficient way to overcome the effect of failures within the network and provide fast restoration of transmission link once a failure has been detected.

Regarding claim 17,

Kawase discloses all the claimed limitations, except (1) wherein the primary and secondary network cables comprise an Ethernet network.

However, in the same field of endeavor, Bray (6,618,392) discloses the selected path in an Ethernet network under IEEE standard 802.3u at processing speed, 100 Mb/s (100 Base-TX over untwisted pairs, 100 Base-FX over fiber optic cabling), see col.1, lines 28-57 (corresponding to (1)). Therefore, it would have been obvious to apply Bray's teaching to Kawase's system with the motivation being to provide faster operation of 100 Base-T system at 125 Mb/s data rate.

Regarding claim 18,

Kawase discloses all the claimed limitations, except (1) wherein the Ethernet network is a 10/100 Base-TX Ethernet network.

However, in the same field of endeavor, Bray (6,618,392) discloses traditional Ethernet network (10Base-T) operate at 10 Mb/s Ethernet protocol, as described in standard IEEE 802.3 and the newer Ethernet network under IEEE

standard 802.3u accomplished the faster operation of 100 Base-T system at 125Mb/s for unshielded twisted pair physical media, i.e., 100 Base-TX, see col.1, lines 28-57 (corresponding (1)). Therefore, it would have been obvious to apply Bray's teaching to Kawase's system with the motivation being to provide faster operation of 100 Base-T system at 125 Mb/s data rate.

Regarding claim 22,

Kawase discloses all the claimed limitations, except (1) wherein the circuit is packaged in a housing of dimensions no greater than five inches high, by ten and one-half inches deep, by eighteen inches wide. However, it would have been obvious to an artisan to change in size to make portable, see In re Rose, 105 USPQ 237 (CCPA 1955).

Regarding claim 23,

Kawase discloses all the claimed limitations, except (1) wherein the circuit may service only a single Ethernet link.

However, in the same field of endeavor, Bray discloses Ethernet networks see fig.1, column 1, lines 22-57 (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Bray's teaching to Kawase's system with the motivation being to provide faster operation at a faster rate.

Regarding claim 26,

Kawase discloses all the claimed limitations, except (1) wherein the circuit is integrated within another Ethernet device to provide automatic redundant network cable operation, or operation with redundant network devices.

However, in the same field of endeavor, Bray discloses switch 24 comprising repeaters 10 Mb/s and 100 Mb/s, see fig.1 (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Bray's teaching to Kawase's system with the motivation being to prevent the network from being rendered unusable by a node or path that is down.

6. Claims 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawase in view of Lo (6,842,481) and Bray (6,618,392) as applied to claim 3 above, and further in view of Takeguchi (6,735,171).

Kawase discloses all the claimed limitations, except (1) wherein the first and second monitoring devices are replaced by one or more programmable logic devices or ASICS.

However, in the same field of endeavor, Takeguchi (6,735,171) discloses a firmware 22, 32, 202, 303 (figs.1, 3, 6, 8, 10, col.3, line 8-col.4, line 10)(corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Takeguchi's teaching to Kawase's system with the motivation being to easy upgrade or modify instructions to how to monitor the path effectively.

7. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawase in view of Lo (6,842,481) as applied to claim 1 above, in view of Burke (6,233,235).

Kawase discloses all the claimed limitations, except (1) wherein the FDDI is a fiber optic 100 base-FX.

However, in the same field of endeavor, Burke (6,233,235) discloses a variety of networks of ATM, SONET, FDDI, as well as 100Base-T Ethernet networks, see column 6, lines 45-48 (corresponding to (1)). Therefore, it would have been obvious to an artisan to apply Burke's teaching to Kawase's system with the motivation being to provide faster operation of 100 Base-T system at 125 Mb/s data rate.

8. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawase in view of Lo (6,842,481) as applied to claim 38 above, and further in view of Wang (6,813,241).

Kawase further discloses when the second monitoring device (signal failure detecting circuit 26-fig.2) indicates a fault in the secondary network cable (protection path), the first monitoring device (signal failure detecting circuit 16-fig.2) indicates no faults in the primary network cable (working path), see figs.9-11.

Kawase discloses all the claimed limitations, except (1) switching the data stream route from the secondary network cable to the primary network cable.

However, in the same field of endeavor, Wang discloses when the working data link 220-fig.5a has recovered from a failure, reversing (switching back) to the working data link from the protection data link (col.8, lines 41-65). Therefore, it would have been obvious to an artisan to apply Wang's teaching to Kawase's system with the motivation being to provide an efficient way to overcome the effect of failures within the network and provide fast restoration of transmission link once a failure has been detected.

9. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang (6,813,241) in view of Lo (6,842,481).

Wang (6,813,241) discloses a circuit (line selection device 260, figs. 5a-5b) enabling the routing of data to a primary (working data link) or secondary (protection data link) network cable connected to primary and secondary nodes (not shown) comprising:

a monitor device 280-fig.5a for monitoring link status of the primary network cable, wherein the link status of the primary network cable includes a notification of a fault within the primary network cable (col.7, lines 10-16);

a complex programmable logic device (CPLD) (not shown) for monitoring the link status (i.e., failure in working data link) reported by the first PHY (based upon the working data link status, triggering event is activated to switch data from failed working data link to the protection data link-emphasis added, col.8, lines 35-38); and

a switch (switch 270-fig.5a) for routing the data to one or the other of the primary or secondary network cables.

Wang's does not explicitly disclose a secondary physical layer transceiver for monitoring the link status of the secondary network cable and secondary node. However, Kawase discloses in figure 2, detecting device 26 for monitoring errors on protection path. Therefore, it would have been obvious to an artisan to apply Kawase's teaching to Wang's system with the motivation being to provide backup to protection path as well as the working path.

Wang discloses all the claimed limitations, except (1) the monitoring devices, each comprising a physical layer transceiver. However, in the same field of the endeavor, Lo (6,842,481) discloses a repeater 30 comprising a physical layer transceiver 36 in figure 2, see also figure 3 (corresponding to

(1)). Therefore, it would have been obvious to an artisan to apply Lo's teaching to Wang's system with the motivation being to provide security in Ethernet based media independent interface communications.

10. Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Lo (6,842,481) and Kawase as applied to claim 44 above, and further in view of Bray (6,618,392).

Wang discloses all the claimed limitations, except (1) the circuit (line selection device 260-fig.5a) comprises a hub device for retransmitting data from a local network port, the hub having a primary and secondary port for both receiving incoming data and sending outgoing data.

However, in the same field of endeavor, Bray (6,618,392) discloses a repeater for retransmitting received data to all ports, see column 1, lines 22-26; fig.1 (corresponding to (1)). Therefore, it would have been obvious to apply Bray's teaching to Wang's system with the motivation being to prevent the network from being rendered unusable by a node that is down.

Allowable Subject Matter

11. Claims 15-16, 35-36 are allowed.

Response to Arguments

12. Applicant's arguments filed 8-31-7 have been fully considered but they are not persuasive.

A/. Applicant argued Kawase does not disclose two cables, a primary cable and a secondary cable, and routing data to one or the other of the primary or second network cables (pages 11-14, remarks).

In reply, applicant is directed to figure 3 wherein a primary cable (working path, fig.3) and a secondary cable (protection path, fig.3), and routing data to one or the other of the primary or second network cables (i.e., for routing data S1-fig.3 from a failure working path to a protection path).

B/. Applicant argued that the cited prior art do not disclose disconnecting from monitoring the primary network cable and primary node

and connected to monitoring the secondary network cable and secondary node when the switching routes the data to the secondary network cable.

In reply, applicant is directed to either figure 2 or 3 wherein a switching 30 for switching the data routing to protection path based upon the error detected on working path, and by switching to the protection path, the monitoring of the working path is disconnected in switching (i.e., on switch or off switch, this feature is well known in the art).

C/. Applicant argued that neither Kawase, Lo, Bray, Burke, Wang, Sterner nor Takeguchi, considered alone or in combination, describes nor suggests an autonomous circuit enabling the routing of data to a primary or secondary network cable connected to primary and secondary nodes (pages 11-14, 19, 21, 23, 27).

First, in response to applicant's arguments, the recitation "an autonomous circuit enabling the routing of data to a primary or secondary network cable connected to primary and secondary nodes" has not been given patentable weight because the recitation occurs in the preamble. A preamble is

generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Second, applicant is directed to figure 3 wherein data S1-fig.3 arriving through a working path 51 at node 52and protection path 61 at node 62-fig.3 to terminating node 73-fig.3 and if there is a failure on the working path, the data would be switched to the protection path, see abstract.

Third, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Fourth, all references' systems are in the same field of detecting error/failure and recovering/protecting data in transmission.

D/. Applicant argued that Kawase does not disclose wherein the logic device routes the signal back to the primary network cable when the first monitoring device indicates a fault in the secondary network cable or secondary node.

In reply, applicant is directed to Kawase-fig.11, wherein Kawase further discloses switching from working to protection path (fig.11, step sp26). Therefore, it would have been obvious to an artisan to implement backup for working path as well as protection path to use as interchangeable with the motivation being to provide protection to the backup/secondary path.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Phuongchau Ba Nguyen whose telephone number is 571-272-3148. The examiner can normally be reached on Monday-Friday from 10:00 a.m. to 6:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on 571-272-3155. The fax

phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Phuongchau Ba Nguyen

/Phuongchau Ba Nguyen/
Examiner
Art Unit 2616

STEVEN NGUYEN
PRIMARY EXAMINER